

# IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA

Universitas Maritim Raja Ali Haji, Fakultas Teknik dan Teknologi Kemaritiman  
Program Studi Teknik Informatika.

2201020098 - Muhammad Rifqi  
2201020123 - Handicap

2201020139 - Muhammad Iqbal Hordani  
2201020101 - Irsyad Widianysyah

## LATAR BELAKANG

Perubahan teknologi jaringan yang berlangsung cepat disertai dengan meningkatnya risiko keamanan siber, seperti pemindaian port, upaya masuk paksa, dan serangan banjir. Risiko-risiko ini dapat berakibat pada kebocoran informasi, gangguan dalam layanan, hingga penguasaan sistem. Untuk itu, diperlukan suatu sistem pengamanan yang bisa mengawasi aliran data jaringan dan mengidentifikasi aktivitas yang mencurigakan secara awal. Intrusion Detection System (IDS) Suricata diimplementasikan sebagai solusi untuk mengenali dan menganalisis potensi serangan pada jaringan secara langsung.

## Tahapan Progres Implementasi Suricata

### Instalasi dan Konfigurasi Suricata

Tahap awal dilakukan instalasi sistem operasi Ubuntu Linux pada mesin virtual. Selanjutnya Suricata diinstal dan dikonfigurasi agar dapat memantau interface jaringan yang digunakan. Direktori log disiapkan dan konfigurasi diuji untuk memastikan Suricata berjalan dengan normal tanpa kesalahan.

### Pembuatan Rule dan Custom Rule

Pada tahap ini dibuat rule dasar dan custom rule untuk mendeteksi berbagai aktivitas mencurigakan, seperti port scanning, brute force SSH, dan ping flood. Rule dirancang menggunakan mekanisme threshold untuk mencegah alert berlebihan (alert flooding).

### Simulasi Serangan Port Scanning (Nmap)

Simulasi port scanning dilakukan menggunakan tools Nmap dengan metode normal scan, SYN scan (-ss), dan aggressive scan (-A). Aktivitas ini mensimulasikan proses pengintaian jaringan oleh penyerang dan berhasil terdeteksi oleh Suricata melalui alert scanning.

### Simulasi Serangan Brute Force Login (Hydra)

Serangan brute force login disimulasikan menggunakan tools Hydra dengan menargetkan layanan SSH. Serangan dilakukan dengan mencoba berbagai kombinasi username dan password secara berulang. Suricata berhasil mendeteksi pola koneksi berulang ke port SSH dan menghasilkan alert brute force.

### Analisis Log Suricata

Log hasil deteksi dianalisis melalui file log Suricata untuk mengevaluasi jenis serangan yang terdeteksi. Analisis menunjukkan bahwa Suricata mampu mengidentifikasi pola serangan scanning, flooding, dan brute force dengan baik.

## KESIMPULAN

Berdasarkan hasil implementasi dan pengujian, Intrusion Detection System (IDS) Suricata terbukti mampu mendeteksi berbagai jenis ancaman keamanan jaringan, seperti port scanning, ping flood, dan brute force SSH. Dengan penggunaan rule dan custom rule yang tepat, Suricata dapat memberikan peringatan dini terhadap aktivitas mencurigakan sehingga membantu administrator jaringan dalam melakukan monitoring dan mitigasi serangan secara efektif.